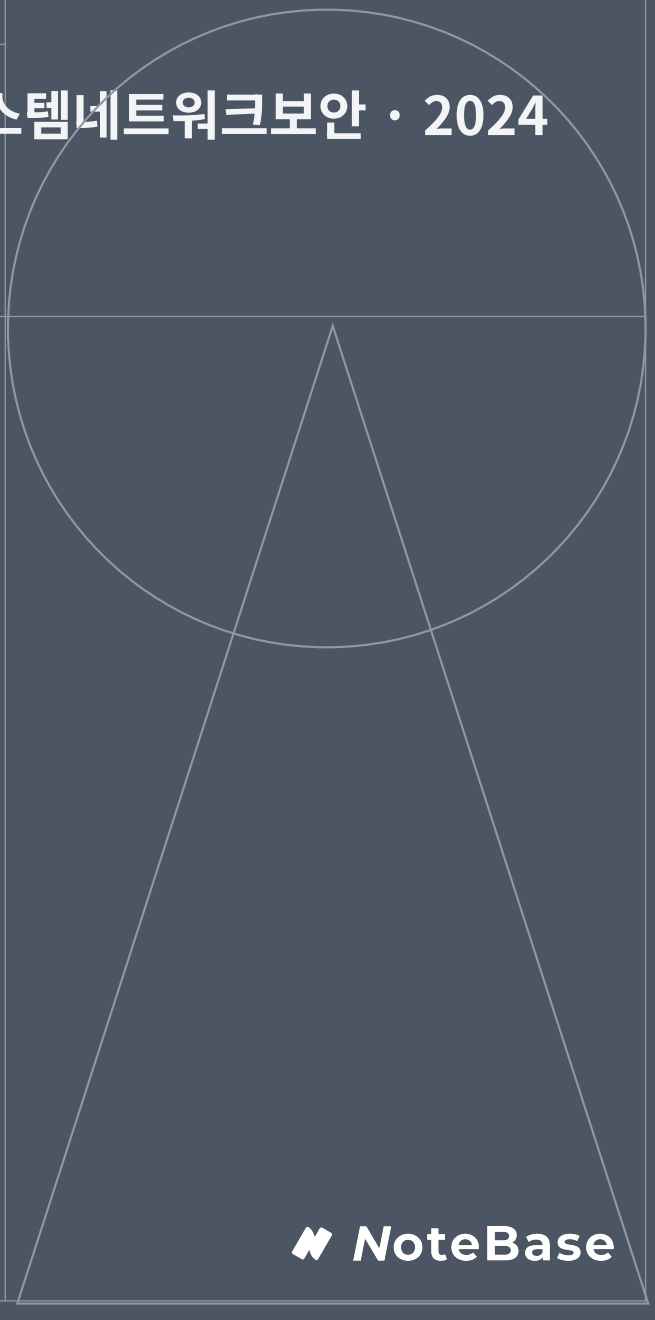
기출OX 해설집

공무원/경찰/경력채용 · 시스템네트워크보안 · 2024



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 시스템네트워크보안 · 2024

공무원/경찰/경력채용 · 시스템네트워크보안 · 2024

문 1. 윈도우(Windows) 서버 보안 설정의 계정 정책에서 암호 정책의 설정 항목으로 가장 적절하지 않은 것은?

① 암호는 복잡성을 만족해야 함

② 최대 암호 길이

③ 최소 암호 사용 기간

④ 최근 암호 기억

정답 2번

간단한 해설

Windows의 기본 암호 정책은 **최소 암호 길이**를 설정한다. '최대 암호 길이'는 해당 기본 정책 항목의 이름이 아니며, 최대 암호 사용 기간과도 구별해야 한다.

선지별 해설

① O. **암호는 복잡성을 만족해야 함**은 암호를 만들거나 변경할 때 복잡성 요구 사항을 적용할지 정하는 정책 항목이다. 계정명 포함 제한과 문자 종류 등의 조건을 통해 단순한 암호 사용을 제한한다.

② X. 기본 암호 정책에는 **최소 암호 길이** 항목이 있으며, '최대 암호 길이'라는 설정 항목은 아니다. 최소 길이는 암호에 필요한 문자 수의 하한을 정한다. 운영체제나 인증 방식에 구현상 길이 한계가 존재하는지와 정책 항목의 이름은 별개의 문제이다.

③ O. **최소 암호 사용 기간**은 사용자가 암호를 바꾼 뒤 다시 변경할 수 있을 때까지의 최소 기간을 정한다. 짧은 시간에 암호를 여러 번 바꾸어 암호 기록 제한을 우회하는 행위를 줄이는 데 이용된다.

④ O. **최근 암호 기억**은 이전에 사용한 암호를 일정 개수만큼 기억하여 재사용을 제한하는 정책 항목이다. 최소 암호 사용 기간과 함께 암호의 반복 재사용을 통제할 수 있다.

따라서 암호 정책의 설정 항목으로 가장 적절하지 않은 것은 ②이다.

NoteBase

문 2. PAM(Pluggable Authentication Module)에 관한 설명으로 가장 적절하지 않은 것은?

① 리눅스(Linux)의 PAM 설정 파일은 /etc/shadow이다.

② FTP, Telnet 등의 일반적인 서비스 인증 설정이 가능하다.

③ 계정의 로그인 시간과 장소 등을 지정하여 제한 설정이 가능하다.

④ 계정이 사용할 시스템 자원에 대한 제한이 가능하다.

정답 1번

간단한 해설

PAM 설정은 보통 **/etc/pam.d/** 또는 **/etc/pam.conf**에서 관리한다. /etc/shadow는 암호 해시와 암호 사용 기간 등의 계정 정보를 저장하므로 PAM 설정 파일과 구별해야 한다.

선지별 해설

① X. Linux-PAM의 설정은 일반적으로 **/etc/pam.d/ 아래의 서비스별 파일** 또는 /etc/pam.conf에서 관리한다. **/etc/shadow**는 암호 해시와 암호 사용 기간 등의 계정 정보를 저장하는 파일이지 PAM 모듈의 적용 순서·조건을 정하는 설정 파일이 아니다. PAM 모듈이 인증 과정에서 shadow 정보를 참조하는 것과 설정 파일의 위치는 구별해야 한다.

② O. PAM을 지원하도록 구현된 서비스는 **서비스별 인증 정책**을 모듈 조합으로 적용할 수 있다. 따라서 FTP나 Telnet 등의 서비스에서도 해당 구현이 PAM과 연동되면 인증 설정을 관리할 수 있다.

③ O. pam_time 같은 모듈로 **로그인 허용 시간**을 제한하고, pam_access 등의 모듈로 사용자·접속 출발지·터미널 조건에 따른 접근을 통제할 수 있다. 여기서 장소는 접속 호스트나 터미널 등 접근 위치 조건의 의미로 이해한다.

④ O. pam_limits 모듈은 사용자 세션에서 **사용 가능한 시스템 자원의 한도**를 적용할 수 있다. 예를 들어 프로세스 수나 열린 파일 수 등의 제한을 계정 또는 그룹별 정책으로 관리한다.

따라서 PAM에 대한 설명으로 가장 적절하지 않은 것은 ①이다.

NoteBase

문 3. 리눅스(Linux)에서 i-node에 저장된 항목으로 가장 적절하지 않은 것은?

① 파일 크기

② 파일의 심볼릭 링크 카운트

③ 파일의 소유자 정보

④ 파일의 속성이 마지막으로 변경된 시간

정답 2번

간단한 해설

i-node의 링크 카운트는 **하드 링크 수**이다. 심볼릭 링크는 별도 파일로 대상을 가리키므로, 심볼릭 링크 카운트라는 ②가 적절하지 않다.

선지별 해설

① O: i-node는 파일을 관리하기 위한 메타데이터를 저장하며, **파일 크기**가 그 항목에 포함된다. 파일 이름과 파일의 내용 자체를 저장하는 위치와는 구별한다.

② X: i-node에 기록되는 링크 수는 **하드 링크 수**이지, 그 파일을 가리키는 심볼릭 링크 수가 아니다. 하드 링크는 같은 i-node를 참조하지만, 심볼릭 링크는 별도의 파일로 경로를 담고 있으므로 대상 파일의 하드 링크 수를 증가시키지 않는다.

③ O: i-node에는 **소유 사용자 ID와 소유 그룹 ID** 등의 소유자 정보가 저장된다. 이 정보는 파일의 접근 권한을 판단하는 데 사용된다.

④ O: i-node에는 **상태 변경 시간인 ctime**이 기록된다. 파일 권한이나 소유자 같은 메타데이터가 변경될 때 갱신되며, 파일 내용 변경 시에도 갱신될 수 있다. ctime은 파일 생성 시간을 뜻하지 않으며, 내용 수정 시간인 mtime과 구별한다.

NoteBase

문 4. 리눅스(Linux)에서 파일권한을 변경함으로써 취약점이 발생할 수 있는 명령은?

① chmod 644 /etc/passwd

② chmod 400 /etc/shadow

③ chmod 666 /etc/hosts

④ chmod 600 /etc/xinetd.conf

정답 3번

간단한 해설

권한 666은 **기타 사용자를 포함한 모두에게 쓰기를 허용**한다. /etc/hosts를 누구나 변경할 수 있으면 이름과 IP주소의 대응 정보가 변조될 수 있다.

선지별 해설

① O(권한 제한이 적절한 쪽). 644는 소유자에게 읽기·쓰기, 그룹과 기타 사용자에게 읽기만 허용한다. /etc/passwd는 계정 식별 정보 등을 조회하는 파일이므로 일반 사용자의 읽기는 통상 허용하되, 쓰기는 소유자로 제한한다. 현대의 섀도 패스워드 구성에서 비밀번호 해시는 별도 /etc/shadow에 저장한다.

② O(접근을 엄격히 제한). 400은 소유자에게만 읽기를 허용한다. /etc/shadow에는 비밀번호 해시 등 민감한 계정 정보가 있으므로 일반 사용자가 읽거나 수정하지 못하게 하는 방향이다. 실제 운영 권한은 배포판의 계정 관리 방식과 정책을 따라야 한다.

③ X(과도한 쓰기 권한). 666은 소유자·그룹·기타 사용자 모두에게 **읽기와 쓰기를 허용**한다. /etc/hosts는 호스트 이름과 IP주소의 대응 정보를 담으므로, 일반 사용자도 이를 변경할 수 있으면 잘못된 주소로 접속을 유도하는 등 보안 문제가 발생할 수 있다. 따라서 취약점을 유발할 수 있는 명령이다.

④ O(권한 제한이 적절한 쪽). 600은 소유자만 읽기·쓰기할 수 있게 한다. /etc/xinetd.conf와 같은 서비스 설정 파일을 비인가 사용자가 열람·변경하지 못하도록 제한하는 설정이다. 여기의 판단은 해당 파일이 정상적으로 관리자 소유라는 전제에서 권한 비트를 비교한 것이다.

NoteBase

문 5. 악성 코드의 유형에 관한 설명으로 가장 적절한 것은?

① 바이러스는 정보를 수집해서 다른 시스템으로 전송하는 악성 코드이다.

② 트로이목마는 악의적인 공격자가 침투하여 사용자의 컴퓨터를 제어하는 악성 코드이다.

③ 애드웨어는 실행 가능한 프로그램을 몰래 변형하여 자신을 복사하는 악성 코드이다.

④ 웜은 잠재적으로 원하지 않은 불필요한 프로그램이란 의미로 치명적인 피해를 주지 않지만 불편함을 주는 악성 코드이다.

정답 2번

간단한 해설

트로이목마는 정상 프로그램처럼 위장한 채 악성 기능을 수행하며, **백도어나 원격 제어 기능**으로 공격자의 시스템 제어를 도울 수 있다. 정보 수집은 스파이웨어, 숙주 파일에 붙는 자기 복제는 바이러스와 구별해야 한다.

선지별 해설

① X: 사용자 정보를 몰래 수집하여 외부 시스템으로 보내는 것은 **스파이웨어**의 대표적인 특징이다. 바이러스의 구별되는 특징은 다른 프로그램이나 파일에 기생하여 자신의 코드를 복제하는 것이다.

② O: 트로이목마는 정상적이거나 유용한 프로그램처럼 위장하여 실행되지만, 내부에는 **악의적인 기능**을 숨긴 프로그램이다. 그 기능으로 백도어나 원격 제어 기능을 제공하여 공격자가 사용자의 컴퓨터를 제어하도록 할 수 있다. 모든 트로이목마의 목적이 원격 제어로 한정되는 것은 아니다.

③ X: 실행 가능한 프로그램을 변형하여 자신을 복사하는 설명은 **바이러스**에 해당한다. 애드웨어는 광고를 표시하거나 광고성 동작을 수행하는 프로그램으로, 숙주 프로그램에 자신을 복제하는 것이 핵심 특징은 아니다.

④ X: 잠재적으로 원하지 않는 프로그램이라는 표현은 **PUP 또는 PUA**를 가리킨다. 웜은 독립적으로 실행되면서 자신을 복제·전파하는 악성 코드이며, 네트워크 자원을 소모하거나 시스템에 큰 피해를 줄 수도 있다. PUP·PUA 역시 항상 무해하다고 단정할 수는 없다.

NoteBase

문 6. 리눅스(Linux)에서 특정 명령어의 절대 경로를 출력하는 명령어로 가장 적절한 것은?

① file

② grep

③ ps

④ which

정답 4번

간단한 해설

실행 파일의 위치를 확인할 때는 **PATH를 검색하는 which**를 사용한다. 파일 형식 판별, 문자열 검색, 프로세스 조회 기능과 구별해야 한다.

핵심 풀이

which는 **PATH에 등록된 디렉터리**에서 지정한 실행 파일을 찾아 경로를 출력한다. 예를 들어 which ls를 실행하면 환경에 따라 /usr/bin/ls와 같은 경로가 나온다. 따라서 실행 파일의 위치를 찾는 명령은 ④ which이다.

file은 파일의 형식을 판별하고, grep은 텍스트에서 패턴과 일치하는 내용을 검색하며, ps는 프로세스 상태를 보여 준다. 이들은 **명령어 실행 파일의 경로 검색**과 목적이 다르다.

NoteBase

문 7. 리눅스(Linux)에서 /etc/passwd 파일에 들어가는 항목으로 가장 적절하지 않은 것은?

① 사용자 ID(uid)

② 그룹 ID(gid)

③ 작업 디렉터리(working directory)

④ 로그인 셸(login shell)

정답 3번

간단한 해설

/etc/passwd에는 사용자 ID, 기본 그룹 ID, **홈 디렉터리**, 로그인 셸 등의 계정 정보가 들어간다. 프로세스의 **현재 작업 디렉터리**를 저장하는 파일은 아니다.

선지별 해설

① O. **사용자 ID(uid)**는 사용자를 수치로 식별하는 값이며 /etc/passwd의 필드에 포함된다. 파일 소유자와 프로세스의 사용자 신원을 구분하는 데 사용된다.

② O. **그룹 ID(gid)**도 /etc/passwd의 필드에 포함되며, 해당 사용자의 기본 그룹을 나타낸다. 사용자가 속한 모든 보조 그룹의 목록을 이 필드에 함께 저장하는 것은 아니다.

③ X. /etc/passwd에 저장되는 디렉터리 항목은 **홈 디렉터리**이지 현재 작업 디렉터리가 아니다. 홈 디렉터리는 계정의 기본 위치이고, 작업 디렉터리는 프로세스가 현재 기준으로 삼는 위치로서 이동에 따라 바뀔 수 있다. 로그인 직후 둘이 같을 수 있어도 서로 다른 개념이다.

④ O. **로그인 셸**은 로그인 시 실행할 명령 해석기 등의 프로그램 경로를 지정하는 필드로 /etc/passwd에 포함된다. 사용자의 로그인 환경을 구성하는 정보이다.

따라서 /etc/passwd 파일의 항목으로 가장 적절하지 않은 것은 ③이다.

NoteBase

문 8. 스택 버퍼 오버플로우 공격에서 함수의 스택 프레임에 들어가는 것으로 가장 적절하지 않은 것은?

① 명령어 레지스터 정보

② 지역 변수 정보

③ 반환 주소 정보

④ 함수 파라미터 정보

정답 1번

간단한 해설

전형적인 함수 스택 프레임에는 지역 변수, 반환 주소, 전달 인자 등이 포함될 수 있다. **CPU의 명령어 레지스터와 스택의 반환 주소**는 서로 다른 개념이다.

선지별 해설

① X. 명령어 레지스터는 CPU가 처리할 명령어를 보관하는 프로세서 내부 요소로, 일반적인 함수 호출에서 **스택 프레임의 기본 구성 항목**으로 설명하지 않는다. 함수가 끝난 뒤 실행을 이어 갈 위치를 저장하는 반환 주소와 혼동하면 안 된다.

② O. 함수의 지역 변수, 특히 지역 배열이나 버퍼는 전형적인 스택 프레임에 저장될 수 있다. 스택 버퍼의 경계를 넘는 쓰기가 발생하면 주변에 있는 다른 데이터가 손상될 수 있다. 다만 최적화 등에 따라 일부 변수는 레지스터에 배치되거나 제거될 수 있다.

③ O. 반환 주소는 함수가 종료된 뒤 **호출한 쪽에서 실행을 재개할 위치**이다. 전형적인 스택 기반 호출 구조에서는 이 주소를 스택에 보관한다. 이는 현재 명령어 자체를 담는 명령어 레지스터와 역할이 다르다.

④ O. 함수에 전달하는 파라미터 정보는 호출 규약에 따라 스택에 놓일 수 있다. 이 문제는 전통적인 스택 프레임 모형을 전제로 하며, 실제 시스템에서는 인자의 일부 또는 전부를 레지스터로 전달하기도 한다. 따라서 모든 호출 규약에서 모든 인자가 반드시 스택에 있다는 뜻은 아니다.

NoteBase

문 9. NIST에서 정의한 클라우드 컴퓨팅의 3가지 서비스 모델과 설명을 가장 적절하게 연결한 것은?

(가) SaaS(Software as a Service)
(나) PaaS(Platform as a Service)
(다) IaaS(Infrastructure as a Service)
㉠ 이용자에게 애플리케이션을 개발, 테스트, 실행하는데 필요한 운영체제, 개발환경, 개발언어 등을 제공하는 서비스이다.
㉡ 이용자에게 클라우드 환경에서 동작하는 애플리케이션/소프트웨어를 제공하는 서비스이다.
㉢ 이용자에게 서버, 스토리지, 네트워크 등의 하드웨어 인프라 자원만을 제공하는 서비스이다.

① (가): ㉠, (나): ㉡, (다): ㉢
② (가): ㉠, (나): ㉢, (다): ㉡
③ (가): ㉡, (나): ㉠, (다): ㉢
④ (가): ㉡, (나): ㉢, (다): ㉠

정답 3번

간단한 해설

SaaS는 **소프트웨어**, PaaS는 **개발·실행 플랫폼**, IaaS는 **기본 인프라 자원**을 제공한다. 이용자가 직접 관리하는 범위와 제공받는 계층을 기준으로 구분한다.

대응 관계 해설

(가) SaaS → ㉡: 이용자가 클라우드에서 실행되는 **완성된 애플리케이션·소프트웨어**를 사용하는 모델이다. 이용자는 소프트웨어의 기능을 이용하며, 기반 서버나 운영체제를 직접 관리하는 것은 아니다.

(나) PaaS → ㉠: 이용자가 애플리케이션을 개발·시험·배포·실행할 수 있는 **플랫폼 환경**을 제공하는 모델이다. 제공자가 지원하는 개발언어, 도구 및 실행 환경을 이용하고, 이용자는 자신이 배포한 애플리케이션을 관리한다.

(다) IaaS → ㉢: 처리 능력, 스토리지, 네트워크 등 **기본 컴퓨팅 자원**을 제공하는 모델이다. 이용자가 그 위에 운영체제와 애플리케이션을 구성할 수 있다. 하드웨어 인프라 자원이라는 표현은 가상화된 자원을 포함하는 서비스 계층의 구분이며, 물리 장비만 직접 제공한다는 뜻은 아니다.

따라서 (가)–㉡, (나)–㉠, (다)–㉢으로 연결한 ③이 적절하다.

NoteBase

문 10. 다음 ㉠에 들어갈 수 있는 용어로 가장 적절한 것은?

2021년 12월 Github에 공개된 공격기법은 (㉠)(이)라는 오픈소스 프로그램이 가지고 있는 취약점을 악용하는 것이다. (㉠)은(는) 아파치 스트럿츠(Apache Struts), 스프링(Spring) 등 각종 웹 프레임워크에서 로그 기록을 위해 사용되는 경우가 많으며, 국내에서는 스프링 프레임워크를 기반으로 한 전자정부 프레임워크 등에서 사용하고 있다.

① Log4j
② HeartBleed
③ LogJam
④ Shellshock

정답 1번

간단한 해설

제시문의 핵심 단서는 **자바 웹 애플리케이션의 로그 기록**과 2021년 12월 공개된 취약점이다. 이는 아파치의 로깅 라이브러리 Log4j와 관련된 설명이다.

빈칸별 해설

㉠은 **Log4j**이다. Log4j는 자바 애플리케이션의 로그 기록에 쓰이는 아파치의 오픈소스 로깅 라이브러리이므로, 제시문의 웹 프레임워크 및 로그 기록이라는 단서에 부합한다. 따라서 ①과 연결된다.

2021년 12월 공개된 대표적 취약점인 **Log4Shell(CVE-2021-44228)**은 영향을 받는 Log4j 2의 JNDI 조회 기능과 관련된다. 공격자가 통제한 입력이 처리되는 조건에서 원격 코드 실행으로 이어질 수 있었다. Log4j는 라이브러리 이름이고, Log4Shell은 그 취약점을 가리키는 이름이라는 점을 구별한다.

NoteBase

문 11. 브로드캐스트(broadcast) 주소를 사용하는 DoS 공격 기법으로 가장 적절한 것은?

① teardrop 공격

② land 공격

③ smurf 공격

④ ping of death 공격

정답 3번

간단한 해설

smurf 공격은 피해자의 주소를 출발지로 위조한 ICMP 요청을 브로드캐스트 주소로 보내, 여러 응답이 피해자에게 집중되도록 하는 DoS 공격이다. 따라서 ③이다.

핵심 풀이

브로드캐스트 주소를 이용한 반사·증폭이 핵심 단서이므로 ③ smurf 공격이다. 피해자의 IP 주소를 출발지 주소로 위조한 ICMP Echo Request를 브로드캐스트 주소로 보내면, 이에 응답하는 여러 호스트의 Echo Reply가 피해자에게 집중될 수 있다. 따라서 브로드캐스트 요청에 대한 다수의 응답이 공격 트래픽을 증폭시키는 구조이다.

teardrop 공격은 **비정상적으로 겹치는 IP 단편** 등을 이용해 재조립 처리의 취약점을 노리는 공격이다.

land 공격은 출발지와 목적지 IP 주소 및 포트를 같게 조작한 패킷으로 취약한 시스템의 처리를 방해한다.

ping of death 공격은 재조립 결과 허용 크기를 넘는 IP 패킷이 되도록 하여 취약한 시스템에 장애를 유발하는 공격이다.

이들은 브로드캐스트 응답의 증폭을 핵심으로 하는 smurf와 구별된다.

NoteBase

문 12. 웹 애플리케이션 해킹을 차단하는 웹 방화벽의 특징으로 가장 적절하지 않은 것은?

① 네트워크 계층에서 동작된다.

② 웹 공격을 탐지하고 차단한다.

③ 동작 방식은 규칙과 애플리케이션 로직을 기반으로 한다.

④ 직접적인 웹 공격 대응 이외에도 정보유출 방지, 부정로그인 방지에 활용할 수 있다.

정답 1번

간단한 해설

웹 방화벽은 HTTP 등의 웹 요청·응답을 분석하는 **응용 계층** 보안 수단이다. 설치 위치가 네트워크 경로라는 이유로 네트워크 계층에서만 동작하는 장비로 보아서는 안 된다.

선지별 해설

① X. 웹 방화벽(WAF)은 웹 요청과 응답의 내용을 해석하는 **응용 계층** 보안 장비 또는 서비스이다. IP 주소 등을 중심으로 처리하는 네트워크 계층 장비로 설명하는 것은 적절하지 않다. 네트워크 경로에 설치될 수 있다는 사실과 검사하는 논리적 계층은 구별해야 한다.

② O. WAF는 **웹 요청·응답을 검사**하여 SQL 삽입이나 크로스 사이트 스크립팅 등 웹 공격의 징후를 탐지하고 정책에 따라 차단한다. 다만 모든 취약점을 자동으로 해결하거나 모든 공격을 완벽히 막는 것은 아니다.

③ O. WAF는 **탐지 규칙과 애플리케이션의 정상 동작에 대한 정책**을 바탕으로 요청의 적절성을 판단할 수 있다. 알려진 공격 패턴이나 허용된 입력 형식·요청 흐름 등을 이용하며, 구체적인 검사 방식은 제품과 설정에 따라 달라진다.

④ O. WAF는 응답에 포함된 민감정보를 검사하거나 로그인 요청의 비정상 패턴을 통제하는 등의 기능으로 **정보유출과 부정로그인 방지**에도 활용될 수 있다. 이러한 효과는 해당 기능과 정책이 구성된 범위에서 기대할 수 있으며, 웹 공격 탐지에만 용도가 한정되는 것은 아니다.

따라서 웹 방화벽의 특징으로 가장 적절하지 않은 것은 ①이다.

NoteBase

문 13. 침해사고 대응팀 CERT(Computer Emergency Response Team)의 역할로서 가장 적절하지 않은 것은?

① 취약점 진단 및 조치

② 개개인에 대한 조사

③ 침해사고 예방 및 전파

④ 침해사고 접수, 분석, 피해 복구

정답 2번

간단한 해설

CERT는 침해사고를 예방하고 사고 발생 시 분석·복구를 담당하는 조직이다. **개개인에 대한 일반적인 조사**는 이러한 기술적 사고 대응의 기본 역할과 구별된다.

선지별 해설

① O: CERT는 시스템의 취약점을 확인하고 패치·설정 개선 등 필요한 조치를 수행하거나 담당 부서와 협조한다. 공격에 악용될 약점을 줄이는 예방 활동에 해당한다.

② X: CERT의 기본 역할은 **정보시스템의 침해사고에 대한 기술적 대응**이지, 개개인의 신상이나 행위를 일반적으로 조사하는 것이 아니다. 사고 원인 분석을 위해 관련 로그를 확인하거나 관계자에게 사실을 물을 수는 있지만, 이를 개인에 대한 일반 조사 업무와 동일시할 수 없다.

③ O: CERT는 보안 위협과 취약점 정보를 수집하여 예방 대책을 마련하고 관련 부서·이용자에게 경보와 대응 정보를 전달한다. 여기서 전파는 **사고 관련 정보와 대응 방안의 공유**를 뜻하며, 침해 행위 자체를 확산한다는 의미가 아니다.

④ O: CERT는 사고 신고를 접수하고 발생 원인과 영향 범위를 분석하며 피해 확산 억제와 서비스·데이터 복구를 지원한다. 접수부터 분석, 복구에 이르는 사고 대응 활동이 핵심 임무이다.

NoteBase

문 14. 스텔스 스캔(stealth scan)에 관한 설명으로 가장 적절한 것은?

① TCP NULL 스캔은 플래그 값을 설정하지 않고 전송하는 스캔 방식이다.

② TCP XMAS 스캔은 해당 포트가 닫혀 있을 때 응답이 없다.

③ TCP FIN 스캔은 해당 포트가 열려 있을 때 RST 패킷으로 응답한다.

④ UDP 스캔은 해당 포트가 열려 있을 때 RST 패킷으로 응답한다.

정답 1번

간단한 해설

TCP NULL 스캔은 **플래그를 하나도 설정하지 않은 패킷**을 보내는 방식이다. FIN·XMAS 스캔의 포트 반응과 UDP의 오류 응답을 TCP RST와 혼동하지 않아야 한다.

선지별 해설

① O: TCP NULL 스캔은 **TCP 제어 플래그를 모두 0**으로 둔 패킷을 전송한다. FIN만 설정하는 FIN 스캔, FIN·PSH·URG를 설정하는 XMAS 스캔과 구별된다.

② X: TCP XMAS 스캔에서 표준적인 TCP 동작을 따르는 닫힌 포트는 **RST로 응답**한다. 응답이 없는 경우는 열린 포트뿐 아니라 필터링된 경우도 포함할 수 있어, 무응답만으로 닫힘이나 열림을 단정해서는 안 된다.

③ X: TCP FIN 스캔의 기본 판별 원리에서는 열린 포트가 패킷을 버리고 **응답하지 않으며**, 닫힌 포트가 RST를 반환한다. 다만 운영체제 구현이나 방화벽에 따라 달라질 수 있으므로 모든 환경에서 이 반응이 보장되는 것은 아니다.

④ X: RST는 **TCP의 제어 플래그**이므로 UDP 포트가 열렸다는 응답으로 사용하지 않는다. UDP 스캔에서는 서비스의 UDP 응답이 열림의 근거가 될 수 있고, 닫힌 포트는 보통 ICMP Port Unreachable로 알려 준다. 무응답은 열림과 필터링을 구별하기 어렵다.

NoteBase

문 15. 침입차단시스템에서 패킷 필터링 시스템에 관한 설명으로 가장 적절하지 않은 것은?

① 하드웨어에 의존하지 않는다.

② 패킷을 조작하는 공격에는 취약하다.

③ 특정 응용프로그램의 취약점이나 기능을 이용하는 공격은 막을 수 없다.

④ 다른 방식에 비해 접근제어 결정에 사용하는 변수의 개수가 많아 고속처리가 불가능하다.

정답 4번

간단한 해설

전통적인 패킷 필터링은 **주소·포트 등 제한된 헤더 정보**로 판단하여 처리 부담이 비교적 작다. 따라서 고속 처리가 불가능하다는 ④가 적절하지 않다.

선지별 해설

① O: 패킷 필터링은 **패킷의 헤더 정보와 규칙을 비교하는 기능**으로, 특정 전용 하드웨어에만 종속되는 방식이 아니다. 라우터 등의 장비뿐 아니라 운영체제의 소프트웨어 기능으로도 구현할 수 있다. 이는 실제 처리 성능까지 하드웨어의 영향을 받지 않는다는 뜻은 아니다.

② O: 전통적인 단순 패킷 필터링은 헤더 정보를 주로 판단하므로, **주소 위조나 단편화 등을 이용해 검사 규칙의 허점을 노리는 공격**에 한계가 있다. 다만 적절한 규칙과 단편 처리로 일부 공격을 차단할 수 있으므로 모든 패킷 조작 공격이 반드시 성공한다는 뜻은 아니다.

③ O: 단순 패킷 필터링은 **응용프로그램의 내용과 동작 의미를 정밀하게 분석하지 않는다.** 따라서 허용된 통신 안에 실린 응용프로그램 취약점 공격을 내용에 근거하여 식별·차단하는 데 한계가 있다. 해당 통신 전체를 주소나 포트 규칙으로 차단하는 것과는 구별한다.

④ X: 패킷 필터링은 주로 **출발지·목적지 주소, 프로토콜, 포트 등 비교적 제한된 헤더 정보**로 접근을 결정하므로, 응용계층의 내용을 깊게 검사하는 방식에 비해 처리 부담이 작아 고속 처리에 유리하다. 변수가 많아 고속 처리가 불가능하다는 설명은 반대이며, 실제 성능은 규칙 수와 구현 등에 따라 달라진다.

NoteBase

문 16. 사설 IPv4 네트워크 주소로 가장 적절하지 않은 것은?

① 10.11.128.0

② 172.30.168.0

③ 169.24.254.0

④ 192.168.192.0

정답 3번

간단한 해설

사설 IPv4 주소는 **10/8, 172.16/12, 192.168/16**의 세 범위에 속한다. 169.24.254.0은 어느 범위에도 포함되지 않는다.

핵심 풀이

RFC 1918의 사설 IPv4 주소 범위는 **10.0.0.0/8**, **172.16.0.0/12**, **192.168.0.0/16**이다. 각각 10.0.0.0~10.255.255.255, 172.16.0.0~172.31.255.255, 192.168.0.0~192.168.255.255에 해당한다.

10.11.128.0은 첫 번째 범위에 포함된다. 172.30.168.0은 두 번째 옥텟 30이 16~31에 속하므로 두 번째 범위에 포함되고, 192.168.192.0은 세 번째 범위에 포함된다.

169.24.254.0은 **세 사설 주소 범위 어느 곳에도 속하지 않는다**. 주소의 마지막 옥텟이 0이라는 사실만으로 사설 주소인지 판단할 수는 없다.

따라서 사설 IPv4 네트워크 주소로 가장 적절하지 않은 것은 ③ 169.24.254.0이다.

NoteBase

문 17. OSI 7계층의 PDU(Protocol Data Unit) 단위가 가장 적절하게 연결된 것은?

① 데이터링크 계층 - 프레임(frame)

② 네트워크 계층 - 세그먼트(segment)

③ 응용 계층 - 데이터그램(datagram)

④ 전송 계층 - 메시지(message)

정답 1번

간단한 해설

데이터링크 계층은 같은 링크를 통해 데이터를 전달하기 위해 **프레임**을 구성한다. 네트워크 계층의 패킷과 전송 계층 TCP의 세그먼트와 구별된다.

선지별 해설

PDU는 특정 프로토콜 계층에서 처리하고 전달하는 데이터 단위이다. 계층별 대표 명칭을 구분하되, 구체적인 프로토콜에 따라 용어가 달라질 수 있다.

① O: 데이터링크 계층의 전송 단위는 **프레임**이다. 상위 계층에서 받은 데이터를 링크에서 전달할 수 있도록 헤더와 필요한 제어 정보를 붙여 프레임으로 구성한다.

② X: 네트워크 계층의 전송 단위는 일반적으로 **패킷**이며, IP에서는 IP 데이터그램이라고도 한다. 세그먼트는 대표적으로 전송 계층의 TCP에서 사용하는 단위이다.

③ X: 응용 계층에서는 응용 프로그램이 주고받는 데이터 또는 메시지를 다룬다. 데이터그램은 대표적으로 IP나 UDP의 전송 단위를 부르는 말이므로, 이 문제의 일반적인 계층별 대응에서 응용 계층과 연결하지 않는다.

④ X: 일반적인 계층별 PDU 분류에서 전송 계층은 **세그먼트**로 설명하며, TCP가 이에 해당한다. UDP의 단위는 데이터그램이라고 한다. 메시지는 이 문제에서 응용 계층 등의 상위 계층 데이터를 가리키는 표현으로 구별한다.

NoteBase

문 18. XSS(Cross Site Scripting) 공격에 사용되는 특수문자로 가장 적절하지 않은 것은?

① <

② &

③ ?

④ ;

정답 4번

출제 포인트

XSS에 관련되는 특수문자의 역할을 비교한다. 이 문항의 O/X는 문자 자체의 사용 가능성에 대한 참·거짓이 아니라, “가장 적절하지 않은 것”으로 선택하는 것이 적절한지에 대한 판단이다.

핵심 개념

XSS는 신뢰할 수 없는 입력이 웹페이지에 포함되어 피해자의 브라우저에서 악성 스크립트로 실행되는 공격이다. 특수문자의 의미와 위험성은 입력이 HTML, JavaScript, URL 중 어느 문맥에 들어가는지에 따라 달라진다.

선지별 해설

① X — <는 HTML 태그의 시작을 나타낸다. 입력이 HTML로 해석되면 태그를 삽입하는 데 이용될 수 있으므로, 이를 가장 적절하지 않은 문자로 고르는 것은 맞지 않는다. 올바른 판단은 “태그 삽입과 관련되는 문자”이다.
② X — &는 HTML 문자 참조의 시작에 쓰인다. 문자 참조를 이용한 표현은 XSS 입력을 인코딩하여 필터를 우회하려는 시도와 관련될 수 있으므로, 가장 적절하지 않은 문자로 고르는 것은 맞지 않는다. 올바른 판단은 “문자 참조와 인코딩 표현에 관련되는 문자”이다.
③ X — ?는 URL에서 쿼리 부분의 시작을 표시한다. 반사형 XSS에서는 URL의 매개변수로 전달된 입력이 응답에 포함되어 실행될 수 있으므로, 공격 입력의 전달과 관련되는 문자이다. 따라서 가장 적절하지 않은 문자로 고르는 것은 맞지 않는다. 올바른 판단은 “URL 쿼리를 통해 입력을 전달하는 데 관련되는 문자”이며, ? 자체가 스크립트를 실행하는 것은 아니다.
④ O — ;는 JavaScript에서 문장 경계를 표시하는 데 쓰인다. 이 문항에서는 <의 태그 시작, &의 문자 참조 시작, ?의 URL 쿼리 시작과 비교하여 ;를 상대적으로 가장 적절하지 않은 것으로 선택한다. 다만 ;도 공격 코드의 문장 구분이나 HTML 문자 참조의 종료에 사용될 수 있으므로, “XSS에 전혀 사용되지 않는다”는 뜻으로 해석하면 틀리다.

오답 포인트

④의 선택을 “세미콜론은 XSS와 무관하다”로 외우면 실제 공격 코드와 충돌한다. 반대로 ③의 ?가 코드 실행 문자가 아니라는 이유만으로 제외하면, URL을 통한 공격 입력 전달이라는 역할을 놓친다.

NoteBase

다시 나오면 이렇게 판단

문자가 태그를 구성하는지, 인코딩 표현을 구성하는지, URL로 입력을 전달하는지, 스크립트 문장을 구분하는지 구별한다. 상대적 적절성을 묻는 문항의 선택 결과를 모든 공격에서 통용되는 사용 가능·불가능의 규칙으로 확대하지 않는다.

암기 포인트

<는 태그 시작, &는 문자 참조 시작, ?는 URL 쿼리 시작, ;는 문장 구분이다. 이 문항의 선택 판단과 실제 공격 문자열에서의 사용 가능성을 구별한다.

NoteBase

문 19. HTTP 프로토콜을 사용하여 웹서버를 공격하는 DDoS 방법으로 가장 적절한 것은?

① SYN Flooding

② ACK Flooding

③ DNS Query Flooding

④ GET Flooding

정답 4번

간단한 해설

GET Flooding은 **HTTP GET 요청**을 과도하게 보내 웹서버의 처리를 방해한다. TCP 제어 패킷이나 DNS 질의를 이용하는 공격과 사용 프로토콜이 다르다.

핵심 풀이

GET Flooding은 **HTTP GET 요청을 대량으로 전송**하여 웹서버의 요청 처리 자원을 소진시키는 공격이다. GET은 웹 자원 조회에 사용하는 HTTP 메서드이므로, HTTP를 이용한다는 단서에 해당하는 것은 ④이다.

SYN Flooding과 ACK Flooding은 **TCP 패킷**을 이용하는 공격이며, DNS Query Flooding은 DNS 질의를 대량으로 보내는 공격이다. 웹서비스에 영향을 줄 수 있다는 사실과 HTTP 요청 자체를 이용한다는 것은 구별해야 한다.

NoteBase

문 20. SNMPv3에서 SNMP 에이전트(agent)가 SNMP 관리자(manager)에게 전송하는 PDU(Protocol Data Unit)의 유형으로 가장 적절한 것은?

① GetRequest

② InformRequest

③ Trap

④ SetRequest

정답 3번

출제 포인트

SNMP PDU의 용도와 전송 방향을 구분하고, 에이전트가 관리자에게 보내는 대표적인 이벤트 통지인 Trap을 식별하는 문제이다.

핵심 개념

SNMP는 관리자가 네트워크 장비의 상태를 조회하거나 설정하고, 에이전트가 장비의 관리 정보를 제공하는 프로토콜이다. PDU는 조회·설정·통지 등의 동작을 담는 메시지 단위이다.
GetRequest는 값 조회 요청, SetRequest는 값 변경 요청이다. Trap은 수신 확인 응답을 요구하지 않는 이벤트 통지이고, InformRequest는 수신 확인 응답을 요구하는 이벤트 통지이다. SNMPv3에서도 Trap과 InformRequest를 사용할 수 있다.

선지별 해설

O/X는 이 문항에서 가장 적절한 선지인지에 대한 선택 판단이다.
① GetRequest — X. 관리자가 에이전트에게 관리 정보의 값을 조회하도록 요청하는 PDU이다. 에이전트가 관리자에게 보내는 통지로 보는 것은 잘못이며, 조회 요청은 관리자에서 에이전트로 전달되고 에이전트는 Response로 응답한다.
② InformRequest — X. 수신자가 Response로 확인하는 이벤트 통지 PDU이다. 에이전트가 관리자에게 보내는 데에도 사용할 수 있으므로 전송 방향 자체가 틀린 것은 아니다. 다만 이 문항의 대표적인 에이전트발 통지를 식별하는 선택으로는 Trap이 더 적절하다. 에이전트의 통지를 모두 InformRequest로 이해하는 대신, 확인 응답이 있는 통지는 InformRequest, 확인 응답이 없는 통지는 Trap으로 구분한다.
③ Trap — O. 에이전트가 장애나 상태 변화 등의 이벤트를 관리자에게 자발적으로 알리는 대표적인 통지 PDU이다. 관리자의 선행 조회 요청 없이 전송할 수 있으며, 통지에 대한 확인 응답을 요구하지 않는다.
④ SetRequest — X. 관리자가 에이전트에게 관리 대상 객체의 값을 변경하도록 요청하는 PDU이다. 에이전트가 관리자에게 보내는 이벤트 통지로 보는 것은 잘못이며, 값 변경 요청의 방향은 관리자에서 에이전트이다.

NoteBase

오답 포인트

② InformRequest도 통지에 사용되므로 에이전트가 보낼 수 없다고 외우면 잘못이다. Trap과 InformRequest의 핵심 차이는 확인 응답의 유무이다. 이 문항에서는 일반적인 에이전트발 통지를 대표하는 Trap을 선택한다.

다시 나오면 이렇게 판단

먼저 조회·설정 요청과 이벤트 통지를 구분한다. 조회 요청이면 GetRequest, 값 변경 요청이면 SetRequest이다. 이벤트 통지는 확인 응답이 없으면 Trap, 확인 응답을 요구하면 InformRequest로 판단한다.

암기 포인트

Get은 조회, Set은 설정, Trap은 확인 없는 통지, Inform은 확인 있는 통지이다.

NoteBase